ClearPath MSP
ClearWatch

COMPARISON GUIDE

from ClearPath MSP

CLEARWATCH COMPARISON GUIDE · KASEYA VSA

Your stack, not theirs.

Kaseya sells VSA as one solution that automates at scale, with AI that drafts workflows. ClearWatch works with the stack you chose, and signs every command.

PUBLISHED NOVEMBER 2026 LENGTH 7 PAGES COMPARES CLEARWATCH AND KASEYA VSA 10

EXECUTIVE SUMMARY

Automation that works with your stack

Kaseya pitches VSA 10 as one solution that automates IT at scale, with Kaseya Assist drafting workflows and FIPS-validated communications. Its one solution means Kaseya's own products, and its workflows run a fix without diagnosing the cause or holding the alert.

ClearWatch automates the step before the fix: a playbook diagnoses each alert before anyone is paged, self-healing holds the page while it works, the tools you already chose are read onto each device, and every command is checked against a signature from a separate authority.

KEY TAKEAWAYS

- **Automation that diagnoses:** the cause, evidence and fix attached to the alert.
- **Your stack, not one vendor's:** Veeam, Cove, Proxmox Backup, SentinelOne, Intune, Keeper.
- **AI inside guard rails:** each assistant signed in as its person, every run signed.
- **Every command signed:** a separate authority signs it, and each machine checks.

IN THIS GUIDE

01 **Automation** — That diagnoses first — 2
02 **One solution** — Or the stack you chose — 3
03 **AI** — Inside guard rails — 4
04 **Every device** — Drawn as it is — 5
05 **Every command signed** — Only in ClearWatch — 6
06 **Side by side** — And how we compared — 7

WHO THIS IS FOR

IT teams and MSPs running Kaseya VSA today, or choosing between the two.

AT A GLANCE

KASEYA'S CLAIMS
Answered
Automation, one solution, AI, security.

EVERY COMMAND SIGNED
ClearWatch only
FIPS protects the channel, not the instruction.

TOOLS YOU CHOSE, READ IN
Six
Veeam, Cove, Proxmox Backup, SentinelOne, Intune, Keeper.

INCLUDED IN CLEARWATCH
Everything here
No add-ons and no second product.

01 AUTOMATION

KASEYA VSA SAYS

> **“Device growth should not force linear growth in manual work.”**
>
> KASEYA.COM/PRODUCTS/KASEYA-VSA, NOVEMBER 2026
>
> VSA's workflows can run a script or restart a service when an alert fires. Nothing attaches the cause to the alert, holds it while the fix runs, or rechecks.

The manual work is finding out why

Most of the manual work behind an alert is the investigation. ClearWatch does it before anyone is paged: a diagnostic playbook runs and the alert arrives with the cause 1, the evidence 2 and the fix 3 attached.

Self-healing holds the page while its fix runs and rechecks, every new client starts with a quiet 14-day baseline, and checks attach themselves where they apply, so growth adds devices, not setup.

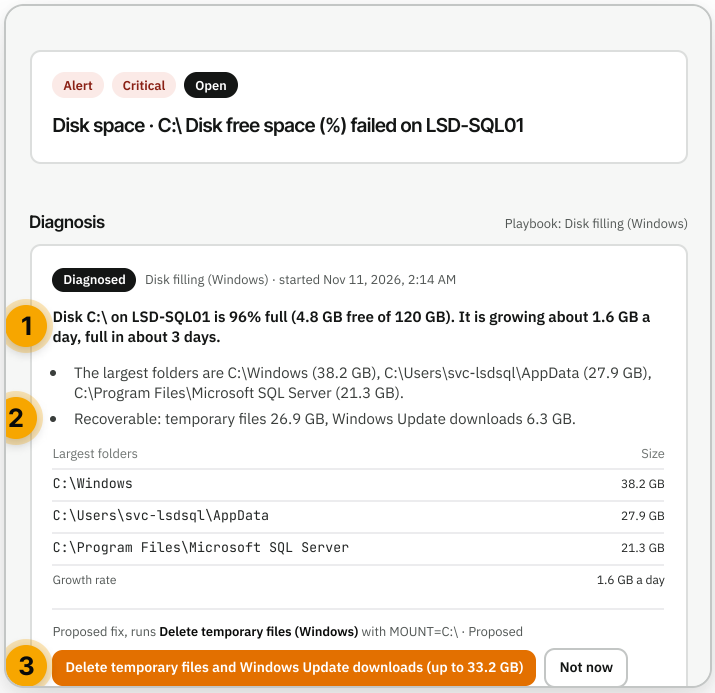


FIGURE 1 An issue on a demo SQL server as it arrives: the cause ClearWatch's playbook worked out, the evidence it read on the machine, and the fix it proposes, run only by a person's press.

From alert to fix

CAPABILITY	CLEARWATCH	KASEYA VSA
Diagnosis before the page A playbook runs first; the alert carries cause, evidence and fix.	✓ **Cause and fix attached**	⊖ Workflows, no diagnosis
Self-healing A fix runs and rechecks while the alert is held.	✓ **Restart or script, then page**	◑ No recheck or hold
Checks only where they apply Checks attach by detected platform, service and role. No filters.	✓ **By role, service, platform**	◑ OS, tags, some server roles
Quiet onboarding baseline A new client learns what is normal before anyone is paged.	✓ **14-day learning period**	⊖ Maintenance windows only
Knows when data stops Each check that stops, gaps or is misconfigured is flagged on its own.	✓ **Missing, gaps, misconfigured**	⊖ Offline alerts only

02 ONE SOLUTION

KASEYA VSA SAYS

“one solution to monitor, manage, automate and support distributed devices”

KASEYA.COM/PRODUCTS/KASEYA-VSA, NOVEMBER 2026

One solution means Kaseya's own products: Datto backup, Datto antivirus and EDR, IT Glue sold separately. VSA reads no Veeam, Cove, SentinelOne, Intune or Keeper.

One console, for the tools you already chose

ClearWatch reads the best-of-breed products you run and puts them on the device they protect: each machine's Veeam, Cove or Proxmox Backup job 3, its SentinelOne agent and threats 1, its Intune compliance and BitLocker key 2.

The credentials ClearWatch itself uses can be read live from Keeper instead of being stored, so changing a password is done in one place.

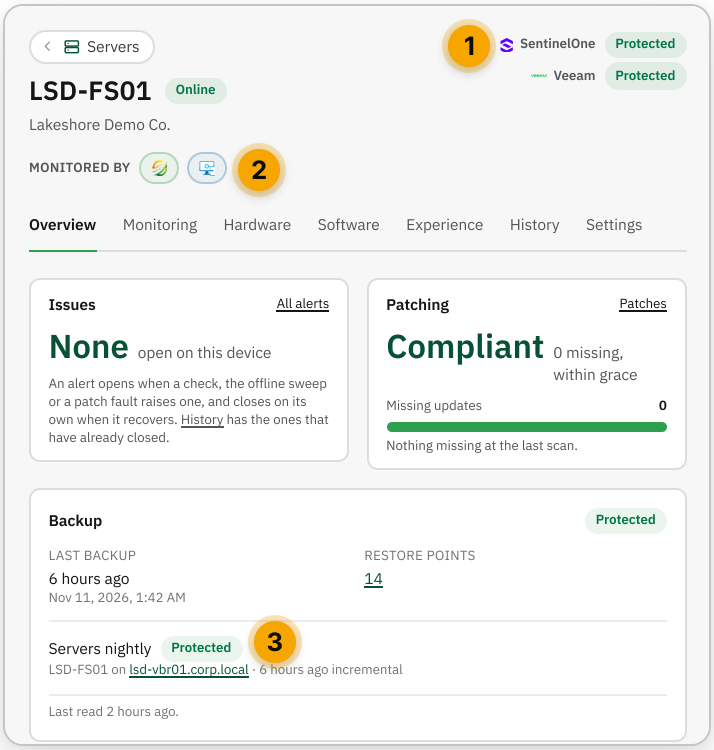


FIGURE 2 One server, three vendors' answers: SentinelOne and Veeam on the title row, Intune under Monitored by, the Veeam job on the Backup card.

Your stack, read in

CAPABILITY	CLEARWATCH	KASEYA VSA
Multi-vendor backup view Several backup vendors' jobs on one dashboard.	✓ **Veeam, Cove, Proxmox Backup** More vendors in development	⊖ Separate Datto views
Backup status per device Each protected machine matched to its device, with alerts.	✓ **Mapped to each device**	⊕ Datto only
SentinelOne Agents, threats and machines missing SentinelOne.	✓ **Threats and coverage gaps**	⊖ Kaseya MDR only
Microsoft Intune Import devices, deploy the agent, read BitLocker keys.	✓ **Import, deploy, BitLocker keys**	⊖ Own MDM instead
Password vault Credentials the RMM uses are read live from Keeper.	✓ **Keeper, read live**	⊖ Session logins only

03 AI

KASEYA VSA SAYS

> **“Describe the automation outcome you need, and Kaseya Assist generates a suggested workflow”**
>
> KASEYA.COM/PRODUCTS/KASEYA-VSA, NOVEMBER 2026
>
> Kaseya Assist drafts a workflow from a prompt for a technician to save. Kaseya's agentic AI is due in early access late 2026, and VSA has no MCP server.

AI that drafts, inside your guard rails

AI assistants such as Claude and ChatGPT connect to ClearWatch today, each signed in as the person using it, and can draft a script into the library with its variables 1 . A secret variable is sealed on the run and withheld once it finishes 2 .

Whatever runs on a machine is still signed by the command authority, under the permission of the person who ran it or a rule a person approved.

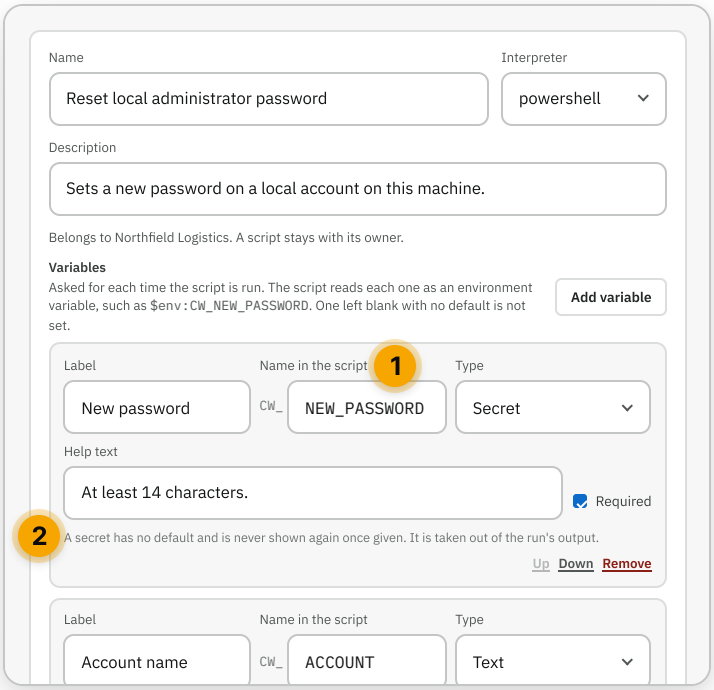


FIGURE 3 Scripts, Library: a client's script open in Edit, with a secret variable and a text variable, rebuilt with demo data.

AI and automation

CAPABILITY	CLEARWATCH	KASEYA VSA
AI assistants (MCP) Claude, ChatGPT and others, each as the person signed in.	✓ **Each person's own sign-in**	⊖ No VSA MCP server yet
Inherited custom fields Values flow down to devices, lockable, with secrets from a vault.	✓ **Lockable, vault secrets**	◑ No vault
API and webhooks A public REST API and outbound webhooks.	✓ **REST API and webhooks**	◑ No webhooks
Incident paging PagerDuty and SolarWinds IR, acknowledgments synced back.	✓ **PagerDuty, SolarWinds IR**	◑ PagerDuty, one-way
Help on every page How-to videos and guides inside the console.	✓ **How-to videos in console**	◑ Help chat

04 EVERY DEVICE

Every device in reach, drawn as it is

Kaseya's help says its site map does not always represent the real layout. ClearWatch's does.

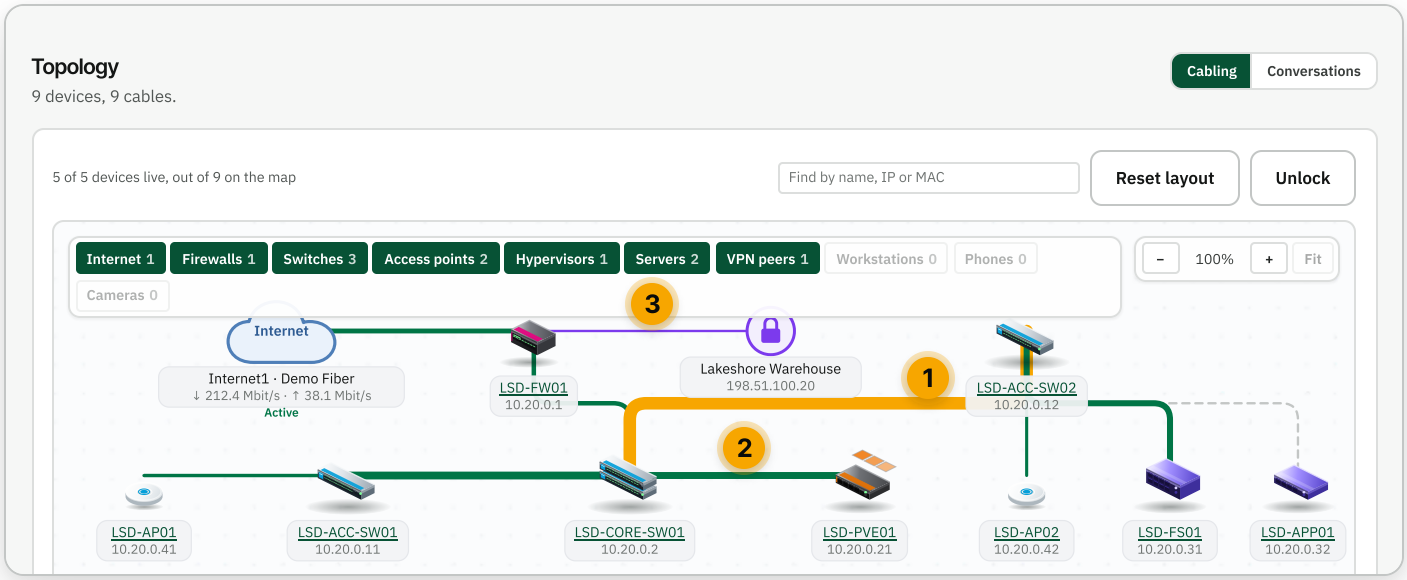


FIGURE 4 Topology, Cabling view: cables drawn from neighbor data, thicker the busier (1), an LACP link (2), a VPN tunnel (3).

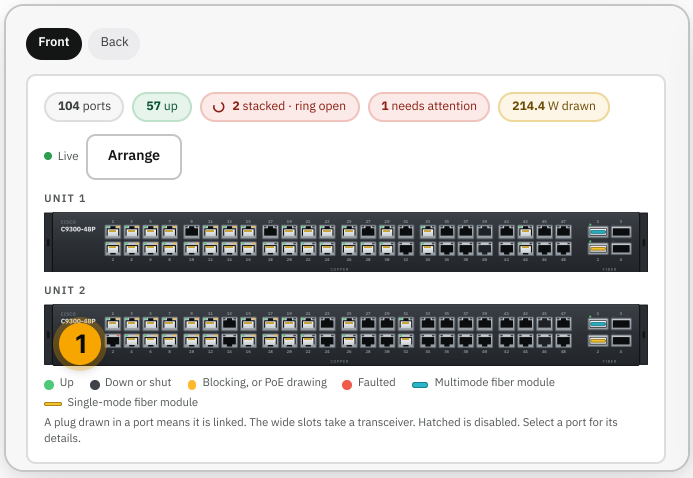


FIGURE 5 Ports, Front: link, PoE and modules per member.

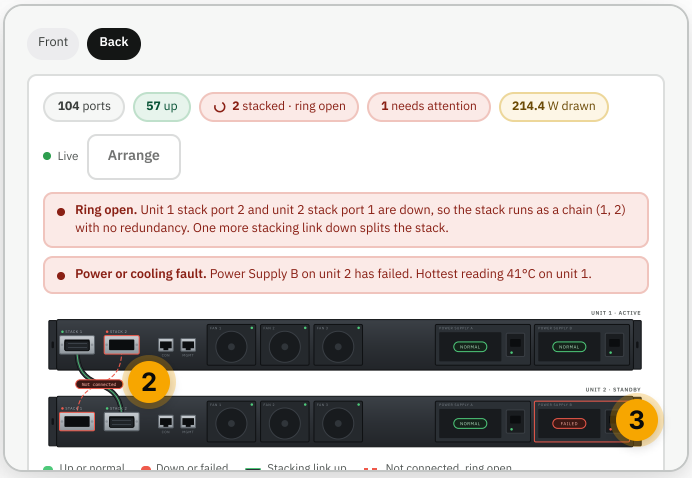


FIGURE 6 Ports, Back: stacking cables, power and fans.

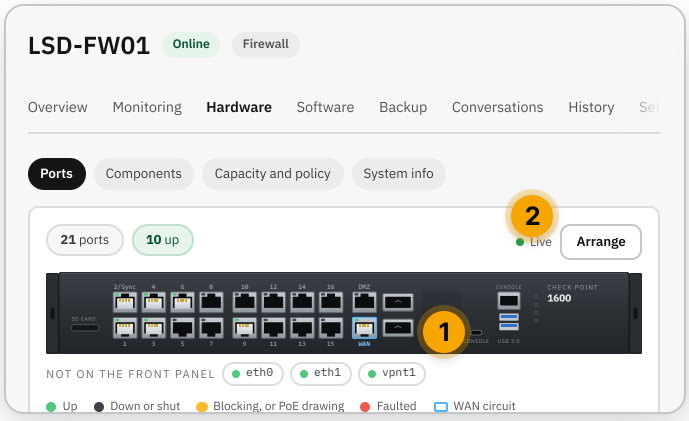


FIGURE 7 LSD-FW01, a Check Point 1600: each socket's link, on its own front.

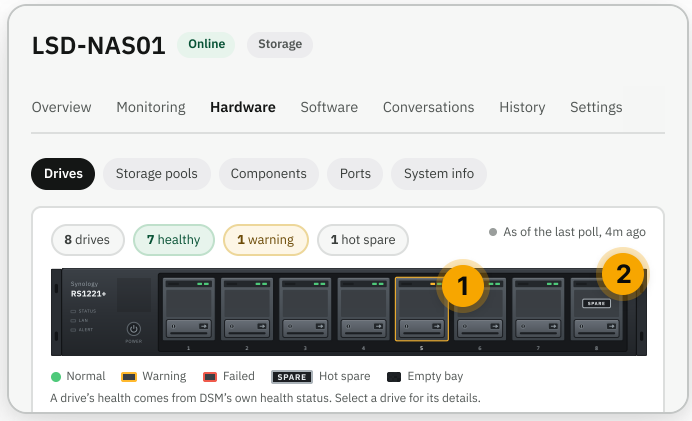


FIGURE 8 LSD-NAS01, a Synology RS1221+: each drive in its bay, one in Warning.

05 EVERY COMMAND SIGNED

> KASEYA VSA SAYS
> **"FIPS 140-3 compliant communications"**
> KASEYA.COM/PRODUCTS/KASEYA-VSA, NOVEMBER 2026

A machine acts only on a signed command

An RMM can run anything on every machine it manages, which makes it the most valuable thing an attacker can reach. ClearWatch takes the power to command machines away from the console itself.

CLEARWATCH CONSOLE
A person asks
Run a script, open a session, install updates, uninstall an agent.

→

COMMAND AUTHORITY
Checked, then signed
A separate service checks that person's own approved permission, then signs with a key held in a hardware security module.

→

THE MACHINE
Verified, or refused
The agent checks the signature against keys built into it, and refuses anything unsigned.

WHAT IT COVERS

- **Everything that changes a machine:** scripts, remote control, the terminal, patch installs, uninstalls and protection settings.
- **A key that never leaves its hardware:** held in a hardware security module, apart from the console's servers.
- **Refused when unsigned:** new agents enforce from the first day.
- **Permissions checked twice:** a raise counts only once another administrator signs it off. Nobody raises themselves.
- **Automation under approved rules:** schedules, self-healing and patch windows run only within rules a person approved.
- **Sessions signed too:** each remote control window and terminal signs its own input.

What Kaseya VSA documents

VSA protects traffic to its agents with FIPS 140-3 validated cryptography and requires two-factor sign-in. It publishes nothing that signs the commands, scripts or sessions it sends, has an agent refuse unsigned work, or stops the agent being uninstalled. Encryption protects the channel. A signature checks the instruction itself.

Every action accounted for

CAPABILITY	CLEARWATCH	KASEYA VSA
Every command signed A separate authority signs each action; the agent refuses anything unsigned.	✓ **Separate authority, HSM key**	⊖ Encrypted transport only
Audited before it runs An action that cannot be logged first is refused.	✓ **Refused if not logged**	◑ Logged after
Installers verify the signer Every install script checks the agent's signature first.	✓ **Every install script**	⊖ Not documented
Agent tamper protection No uninstall without a code from the console, set per client.	✓ **Uninstall code, per client**	⊖ Settings password only
Client-controlled access A client can refuse or withdraw a provider's access.	✓ **Client can refuse**	⊖ MSP-controlled

06 SIDE BY SIDE

Kaseya VSA and ClearWatch: all 40 capabilities

Included · Partial · Add-on · Not offered or not documented

CAPABILITY	CW	VSA
Quiet onboarding baseline	✓	Maintenance windows only
Diagnosis before the page	✓	Workflows, no diagnosis
Knows when data stops	✓	Offline alerts only
Checks only where they apply	✓	OS, tags, some server roles
Outage-first routing	✓	Severity filters only
End-user experience score	✓	No score
Agentless with failover	✓	One probe, no failover
Switch config history	✓	Not documented
Browser SSH to devices	✓	Enrolled devices only
Cabling topology map	✓	Scan map
Switch front and back views	✓	Not documented
Storage drive-bay view	✓	Free space only
Built-in IPAM	✓	Not documented
Controllers and cameras	✓	Not documented
Windows and third-party apps	✓	Third-party licensed
Linux patching	✓	Per device, not policy
Several install rounds per window	✓	One pass
Owed-restart ledger	✓	Pending state
Self-healing	✓	No recheck or hold
Inherited custom fields	✓	No vault

CAPABILITY	CW	VSA
Every command signed	✓	Encrypted transport only
Audited before it runs	✓	Logged after
Update lockdown verified	✓	Set, not verified
Installers verify the signer	✓	Not documented
Agent tamper protection	✓	Settings password only
Remote control	✓	Included
Recording by client policy	✓	Windows only, no default
Support without an agent	✓	Windows and macOS
Searchable terminal recordings	✓	Not documented
Multi-vendor backup view	✓	Separate Datto views
Backup status per device	✓	Datto only
SentinelOne	✓	Kaseya MDR only
Microsoft Intune	✓	Own MDM instead
Password vault	✓	Session logins only
Client-controlled access	✓	MSP-controlled
AI assistants (MCP)	✓	No VSA MCP server yet
API and webhooks	✓	No webhooks
Incident paging	✓	PagerDuty, one-way
Co-managed IT	✓	Org-scoped teams
Help on every page	✓	Help chat

How we compared. Each vendor's own public documentation, release notes, product and pricing pages, checked October and November 2026; quotes are from Kaseya VSA's own pages as of November 2026. Included means it does what ClearWatch does, in the RMM itself, at no extra license; Partial covers part of it; Add-on needs a separately licensed product or tier; Not documented means we found no public documentation, not that the vendor cannot do it. Every cell is backed by a source, available on request. Screens are rebuilt from the ClearWatch console with demo data.

Running Kaseya VSA today?

Start a free trial, or ask us to walk you through ClearWatch on your own devices.

clearwatch.com

ClearWatch™ is a trademark of ClearPath MSP. Kaseya, VSA, Kaseya 365, Kaseya Assist, Datto and IT Glue are trademarks of Kaseya. All other names are trademarks of their respective owners.